



PRIVACY POLICY

Last updated 16 Nov 2021

Elements of this policy have been modelled on the Caritas Australia Privacy Policy. The REACH for Nepal foundation expresses its thanks to Caritas for making this resource available.

Purpose of this Policy

This document outlines the REACH for Nepal (RFN) Privacy Policy. This policy meets the Australian Privacy Principles and complies with the Privacy Act 1988 (Privacy Act) in relation to the Foundation's collection and use of personal information.

The purpose of this document is to outline the ways RFN handles and protects the confidentiality of personal information provided to the Foundation.

The policy applies to all associated with the foundation here in Australia and in Nepal.

Context

There are 13 [Australian Privacy Principles](#) which govern standards, rights and obligations around:

- the collection, use and disclosure of [personal information](#)
- an organisation or agency's governance and accountability
- integrity and correction of personal information
- the rights of individuals to access their personal information

Policy Commitments

Why we collect information

We commit to only collecting personal information that is required for activities relating to the Foundation's volunteer work and to always collect information fairly and transparently. When collecting personal information, we will ensure to clearly communicate with you the need for this information, how we intend to use it and how



it will be stored to protect your privacy. Information will only be obtained directly from you with your consent, as far as practicable.

For prospective staff, personal information may be sought by speaking with referees, including previous employers who may not have been nominated as referees.

We will also collect information from our partners including names and addresses so that we are able to conduct background checks (such as counter-terror finance checks).

We collect personal information of volunteers and donors such as names, addresses and phone numbers, email addresses and details and details of communication preferences. This information allows us to manage volunteer and donation lists, send newsletters to supporters, and provide supporting evidence when seeking grants and other government funding. We may use personal information to send promotional or marketing material from time-to-time. Any such material will clearly indicate to the receiver how they may opt out of receiving such material in the future.

We do not store credit card details. We use a third party as a payment gateway to our bank account.

Volunteers will also be required to provide their personal information when applying for a Working with Vulnerable People card; however, this is at the volunteers discretion – the Foundation will only request confirmation that a prospective or current volunteer has been granted to hold this check. This may include photographic proof of the card and the personal information contained therein.

Our website uses cookies and other digital identifiers that provide information on how the site is used. Users can clear or disable cookies or digital identifiers from their device by changing security settings on their web browser. However, doing this may impact their experience and functionality of the website.

How we collect information

RFN collects personal information directly from you when you provide it through email, the RFN web-site, on-line forms or via the phone.

Anonymity

If you wish, you can remain anonymous or use a pseudonym when you contact us and if you make a donation. We will respect your anonymity. However, if you choose not to provide us with your personal information, we may not, for example, be able to provide you with an official tax-deductible receipt or a letter of thanks, and we may not be able to assist you fully with your query or complaint.



How we use your information

We do not use or disclose personal information that we have collected for any reason other than the primary purpose for which it was collected, unless:

- you have provided consent for us to use it for another purpose
- the purpose is closely related to the primary purpose, or
- we are legally required to use the information

We will ask for consent from a supporter before publishing any information about their donation.

How we store your information

We are committed to securely storing personal information.

The Foundation is run entirely by volunteers and does not operate in any one single physical location. Nearly all the personal information we collect is through electronic means and is therefore stored electronically. Cyber risks are actively managed through the Operational Risk Management Plan. There are exceptional situations where personal information may need to be printed and when this is required, all printed documents will be securely stored in a locked filing cabinet.

Security measures include but are not limited to:

- all personal and sensitive information is securely stored at all times
- for electronic information, virus scanning tools are frequently used
- all virtual databases are protected by secure user ID and passwords
- only authorised people will have access to personal information
- email protocols are used (such as BCC so recipients can't see email addresses of other recipients)
- confidentiality and privacy clauses are included in all contracts
- all cloud-based storage meets privacy requirements
- third party providers are required to have security measures in place

Personal details (name, address, contact phone number, date of birth) are shared with our planning and delivery partner in Nepal (REACH for Nepal – Nepal Charter) for them to organise passes to National Parks and internal travel and accommodation arrangements.

Accessing the information we collect

You may be able to obtain a copy of personal information that we hold about you. To make a request to access this information please contact us in writing to [Manager Communications and Company Secretary](#).



There are circumstances under Australian privacy laws where access to the personal information cannot be granted. For example, when it would unreasonably affect someone else's privacy, or pose a serious threat to another person's life, health or safety.

If you notice any errors in the use, storage or disclosure of your personal information, we will take all reasonable steps to correct it.

If you request access to information you may need to provide proof of identity before information is disclosed.

If we cannot give you access to personal information, we will tell you the reason why.

Opt out option of mailing

When we send you marketing materials (whether by post, email or telephone), we will provide you with an opportunity to opt-out (unsubscribe) to future communications. By electing not to opt-out, we will assume we have your implied consent not to receive similar communications in the future.

If you wish to opt-out, please select the option to opt out in our newsletters, email [Manager Communications and Company Secretary](#), phone +61 2 8405 7950 or write to us via post at PO Box 76 Calwell ACT 2905.

Roles and Responsibilities

At RFN, we recognise that a culture of protecting privacy starts with strong leadership.

The Board of Directors is responsible for:

- Ultimate accountability for our organisational policies
- Guiding the governance and culture of RFN through strategic leadership
- Demonstrating a commitment to a culture of protecting privacy and leading by example
- Approving and regularly reviewing this policy in holding the Leadership Team accountable to how effectively this policy is implemented and adhered to
- Investigating very serious complaints and providing a response

The Chief Executive Officer is responsible for:

- Ensuring this policy is upheld and regularly reviewed
- Demonstrating a commitment to a culture of protecting privacy and leading by example
- Informing the Board of any concerns relating to complaints that may present risk to RFN or its personnel

- Ensuring all senior employees are accountable to this policy

Executive Team members are responsible for:

- Demonstrating a commitment to a culture of protecting privacy and leading by example
- Ensuring our procedures, practices, plans and operations align with and adhere to this policy
- Reporting to the Board via the CEO on any privacy policy matters or potential breaches
- Ensuring their team are aware of this policy and understand their responsibilities
- Ensuring this policy is publicly available via the web-site
- Monitoring and responding to any complaint that is assigned to them to investigate.

Managers are responsible for:

- Demonstrating a commitment to a culture of protecting privacy and leading by example
- Communicating this policy and related procedures to other volunteers

All associated with the RFN foundation are responsible for:

- Understanding and following this policy and related procedures
- Ensuring that actions are in line with this policy, and that all work reflects the guiding principles and policy commitments above
- Not encouraging others (directly or indirectly) to breach this policy
- Reporting any breach to an appropriate manager. For any sensitive complaints, reports should be made to the [CEO](#)

Administration of this Policy

This policy is administered by the Manager Communications and Company Secretary and will be fully reviewed every 3 years.